Title Page

Smart Card Technology – A Tutorial

Main Menu

- Overview
- Technology Review
- Applications
- Featured Articles and Topics

SECTION 1: OVERVIEW

Scene 1.1: Section Objectives

In this section we will examine:

- The evolution of the smart card
- Types of smart cards in the market place, and
- Historical milestones.

Scene 1.2: Introduction

Imagine the power of a computer, the speed and security of electronic data, and the freedom to carry that information anywhere on earth. Imagine a computer so small it fits inside a plastic card like the credit card you carry in your wallet. Imagine the Smart Card.

Scene 1.3: Computer Evolution

Information technology is evolving at an amazing pace. Personal computers, fax machines, pagers, and cell phones are in the hands of millions of people worldwide. Similarly, interest in smart card technology has soared in the 1990's, and by the year 2000 the number and variety of smart card-based applications will explode around the world.

Scene 1.4: Smart Card Evolution

The driving factors of the growing interest in smart cards include the declining cost of smart cards and the growing concern that magnetic stripe cards can not provide the protections necessary to thwart fraud and security breaches. This security issue alone may propel smart card technology to the forefront of business transactions.

Scene 1.5: What is a Smart Card?

What is a smart card? The term *Smart Card* is loosely used to describe any card with a capability to relate information to a particular application such as magnetic stripe, optical, memory, and microprocessor cards. It is more precise, however to refer to memory and microprocessor cards as smart cards.

- A magnetic stripe card has a strip of magnetic tape material attached to its surface. This is the standard technology used for bank cards.
- Optical cards are bank card-size, plastic cards that use some form of laser to write and read the card.
- Memory cards can store a variety of data, including financial, personal, and specialized information; but cannot process information.
- Smart cards with a microprocessor look like standard plastic cards, but are equipped with an embedded Integrated Circuit (IC) chip. Microprocessor cards can store information, carry out local processing on the data stored, and perform complex calculations. These cards take the form of either "contact" cards which require a card reader or "contactless" cards which use radio frequency signals to operate.

Scene 1.6: Microprocessor Smart Card

For the purpose of this tutorial, we are focusing our discussion on the microprocessor type of *Smart Card* defined as an IC chip contact card with a microprocessor and memory. No bigger than a credit card, this smart card contains a dime-sized microchip that can process and store thousands of bits of electronic data. Unlike passive devices (such as a memory card or magnetic stripe card) that can only store information, the smart card is active and able to process data in reacting to a given situation. This capability to record and modify information in its own non-volatile, physically protected memory makes the smart card a powerful and practical tool. Smart cards are small and portable; they can interact with computers and other automated systems; and the data they carry can be updated instantaneously.

Scene 1.7: Historical Milestones

Although considered a leading edge technology, IC contact cards, an original French invention, have been with us for over 20 years. Since the 1970s, the history of smart cards has reflected steady advances in chip capabilities and capacity, as well as increases in the number and variety of applications.

Click on the dates below to review the historical milestones in the development of smart card technology.

1970 Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept.

1974 Roland Moreno of France filed the original patent for the IC card, later dubbed the "smart card".

1977 Three commercial manufacturers, Bull CP8, SGS Thomson, and Schlumberger began developing the IC card product.

1979 Motorola developed the first secure single chip microcontroller for use in French banking.

1982 Field testing of serial memory phone cards took place in France--the world's first major IC card test.

1984 Field trials of ATM bank cards with chips were successfully conducted.

1986 In March, 14,000 cards equipped with the Bull CP8 were distributed to clients of the Bank of Virginia and the Maryland National Bank. Also, 50,000 Casio cards were distributed to clients of the First National Palm Beach Bank and the Mall bank.

1987 First large-scale smart card application implemented in the United States with the U.S. Department of Agriculture’s nationwide Peanut Marketing Card.

1991 First Electronic Benefits Transfer (EBT) smart card project launched for the Wyoming Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).

1992 A nationwide prepaid (electronic purse) card project (DANMONT) was started in Denmark.

1993 Field test of multi-function smart card applications in Rennes, France, where the Telecarte function (for public phones) was enabled in a Smart Bank Card.

1994 Europay, MasterCard, and Visa (EMV) published joint specifications for global microchip-based bank cards (smart cards).

Germany began issuance of 80 million serial memory chip cards as citizen health cards.

1995 Over 3 million digital mobile phone subscribers worldwide begin initiating and billing calls with smart cards.

First of 40,000 multi-functional, multi-technology MARC cards with chips were issued to U.S. Marines in Hawaii.

1996 Over 1.5 million VISACash stored value cards were issued at the Atlanta Olympics.

MasterCard and Visa began sponsorship of competing consortia to work on solving the problems of smart card interoperability; two different card solutions were developed: the JavaCard backed by Visa, and the Multi-application Operating System (MULTOS) backed by MasterCard.

1998 In September 1998, the U.S. Government's General Services Administration and the United States Navy joined forces and implemented a nine-application smart card system and card management solution at the Smart Card Technology Center in Washington, DC. The Technology Center's primary purpose is to demonstrate and evaluate the integration of multi-application smart cards with other types of technology, showcasing systems available for use in the Federal Government.

Microsoft announced its new Windows smart card operating system.

France began piloting a smart health card for its 50 million citizens.

1999 The U.S. Government's General Services Administration has been involved in the Smart Access Common ID Project for the past year. The Smart Access Common ID Card program will establish a contract vehicle for use by all Federal agencies to acquire a standard, interoperable employee identification card, from one or more vendors, capable of providing both physical and logical (system/network) access to all Federal employees.

The United States Government (General Services Administration) began a true multi-application Java card pilot in the Washington, DC, metropolitan area.

Scene 1.8: How Many Cards?

Today, smart cards are used by millions of cardholders worldwide and are at work in more than 90 countries, primarily in Europe and the Far East, processing point-of-sale transactions, managing records, and protecting computers and secure facilities.

This completes the Overview. Return to the Main Menu and select the next topic.

SECTION 2: TECHNOLOGY REVIEW

Scene 2.1: Section Objectives

In this section we will review:

- Smart card microchip technology
- The chip operating system
- Key features and characteristics, and
- International Standards.

Scene 2.2: The Micromodule

Smart cards are credit card-sized, often made of flexible plastic (polyvinyl chloride or PVC), and are embedded with a micromodule containing a single silicon integrated circuit chip with memory and microprocessor. The micromodule has eight metallic pads on its surface, each designed to international standards for VCC (power supply voltage), RST (used to reset the microprocessor of the smart card), CLK (clock signal), GND (ground), VPP (programming or write voltage), and I/O (serial input/output line). Two pads are reserved for future use (RFU). Only the I/O and GND contacts are mandatory on a card to meet international standards; the others are optional.

Scene 2.3: The Micromodule

When a smart card is inserted into a Card Acceptance Device or CAD (such as a point-of-sale terminal), the metallic pads come into contact with the CAD’s corresponding metallic pins, thereby allowing the card and CAD to communicate. Smart cards are always reset when they are inserted into a CAD. This action causes the smart card to respond by sending an “Answer-to-Reset “ message, which informs the CAD, what rules govern communication with the card and the processing of a transaction.

Scene 2.4: Micromodule Components

The micromodule on board the smart card is made up of certain key components that allow it to execute instructions supporting the card’s functionality. Click each component in the diagram for an explanation.

The **Microprocessor Unit (MPU)** executes programmed instructions. Typically, older version smart cards are based on relatively slow, 8-bit embedded microcontrollers. The trend during the 1990s has been toward using customized controllers with a 32-bit Reduced Instruction Set Computing (RISC) processor running at 25 to 32 MHz.

The **I/O Controller** manages the flow of data between the Card Acceptance Device (CAD) and the microprocessor.

Read Only Memory (ROM) or Program Memory is where the instructions are permanently burned into memory by the silicon manufacturer. These instructions (such as when the power supply is activated and the program that manages the password) are the fundamentals of the Chip Operating System (COS) or, as often called, the “Mask.”

Random Access Memory (RAM) or Working Memory serves as a temporary storage of results from calculations or input/output communications. RAM is a volatile memory and loses information immediately when the power supply is switched off.

Application Memory, which today is almost always double E-PROM (Electrically Erasable Programmable Read-Only Memory) can be erased electronically and rewritten. By international standards, this memory should retain data for up to 10 years without electrical power and should support at least 10,000 read-write actions during the life of the card. Application memory is used by an executing application to store information on the card.

Scene 2.5: What is the COS?

The smart card's Chip Operating System (frequently referred to simply as COS; and sometimes referred to as the Mask) is a sequence of instructions, permanently embedded in the ROM of the smart card. Like the familiar PC DOS or Windows Operating System, COS instructions are not dependent on any particular application, but are frequently used by most applications.

Chip Operating Systems are divided into two families:

- The general purpose COS which features a generic command set in which the various sequences cover most applications, and
- The dedicated COS with commands designed for specific applications and which can even contain the application itself. An example of a dedicated COS would be a card designed to specifically support an electronic purse

application.

Scene 2.6: What is the COS?

The baseline functions of the COS which are common across all smart card products include:

- Management of interchanges between the card and the outside world, primarily in terms of the interchange protocol.
- Management of the files and data held in memory.
- Access control to information and functions (for example, select file, read, write, and update data).
- Management of card security and the cryptographic algorithm procedures.
- Maintaining reliability, particularly in terms of data consistency, sequence interrupts, and recovering from an error.
- Management of various phases of the card's life cycle (that is, microchip fabrication, personalization, active life, and end of life).

Scene 2.7: Key Features and Characteristics

Shown below are some of the key features and characteristics of smart cards. Click on each feature for a description.

Cost

Typical costs range from $2.00 to $10.00. Per card cost increases with chips providing higher capacity and more complex capabilities; per card cost decreases as higher volume of cards are ordered.

Reliability

Vendors guarantee 10,000 read/write cycles. Cards claiming to meet International Standards Organization (ISO) specifications must achieve set test results covering drop, flexing, abrasion, concentrated load, temperature, humidity, static electricity, chemical attack, ultra-violet, X-ray, and magnetic field tests.

Error Correction

Current Chip Operating Systems (COS) perform their own error checking. The terminal operating system must check the two-byte status codes returned by the COS (as defined by both ISO 7816 Part 4 and the proprietary commands) after the command issued by the terminal to the card. The terminal then takes any necessary corrective action.

Storage Capacity EEPROM: 8K – 128K bit. (Note that in smart card terminology, 1K means one thousand bits, not one thousand 8-bit characters. One thousand bits will normally store 128 characters, the rough equivalent of one sentence of text. However, with modern data compression techniques, the amount of data stored on the smart card can be significantly expanded beyond this base data translation.)

Ease of Use Smart cards are user-friendly for easy interface with the intended application; handled like the familiar magnetic stripe bank card.

Susceptibility Susceptible to chip damage from physical abuse, but more difficult to disrupt or damage than the magnetic stripe card.

Security Smart cards are highly secure. Information stored on the chip is difficult to duplicate or disrupt, unlike the outside storage used on magnetic stripe cards that can be easily copied. Chip microprocessor and Co-processor supports DES, 3-DES, RSA or ECC standards for encryption, authentication, and digital signature for non-repudiation.

First Time Read Rate ISO 7816 limits contact cards to 9600 baud transmission rate; some Chip Operating Systems do allow a change in the baud rate after chip power up; a well designed application can often complete a card transaction in one or two seconds.

Speed of Recognition Smart cards are fast. Speed is only limited by the current ISO Input/Output speed standards.

Proprietary Features These include Chip Operating System and System Development Kits.

Processing Power Older version cards use an 8-bit micro-controller clockable up to 16 MHz with or without co-processor for high-speed encryption. Current trend is toward customized controllers with a 32-bit RISC processor running at 25 to 32 MHz.

Power Source

Mostly 5 volt DC power source.

Support Equipment Required

For most host-based operations, only a simple Card Acceptance Device (that is, a card reader/writer terminal) with an asynchronous clock, a serial interface, and a 5-volt power source is required. For low volume orders, the per unit cost of such terminals runs between $100 and $250, the cost decreasing significantly with higher volumes. More costly Card Acceptance Devices are hand-held, battery-operated terminals and EFT/POS desktop terminals.

Scene 2.8: ISO 7816 Standards

Standards are key to ensuring interoperability and compatibility in an environment of multiple card and terminal vendors. Integrated circuit card standards have been underway since the early 1980's on both national and international levels. Basic worldwide standards for smart cards have been and continue to be established by the International Organization for Standardization, which has representation from over 70 nations. The ISO 7816 series is the international standard for integrated circuit cards.

International Organization for Standards Smart Card Standards

Part Number	Date Approved	General Description
7816-1	1987	Governs the physical dimensions of the card (width, length, and thickness), which are those of a standard credit card.
7816-2	1988	Governs the dimensions and locations of the chip contacts.
7816-3	1989 with two amendments in 1992 and 1994	Governs the electronic signals and transmission protocols in terms of electrical characteristics, transmission protocols, and the format of the card "Answer to Reset".
7816-4	In Progress	Governs inter-industry commands and responses to include the Application Protocol Data Unit (the command exchange format independent of the transfer protocol), historical characters of the Answer to Reset, file structures and access methods, data object oriented commands, and a secure messaging format.

7816-5	1994 with one amendment in progress	Provides for a registration system for application identifiers, which allow terminals to select unambiguously an application in a card.
7816-6	1996	Governs data elements for interchange.
7816-7	1999	Governs Smart Card Query Language. Commands to support a relational database on a card.
7816-8	In Progress	Governs security related inter-industry commands.
7816-10	In Progress	Governs synchronous cards.

Scene 2.9: COS Standards

Although smart cards conform to a set of international standards, there is currently no standard Chip Operating System, or anything as common as Microsoft's Windows, or UNIX. Each smart card vendor provides the market with a distinct product. The key discriminator among smart card products is the proprietary operating system each offers to the customer.

Scene 2.10: Work of Other Industry Standard Groups

Other standards groups and vendor consortia are working on standards proposals and specifications that will have impact on smart cards. Shown below is a review of their activities.

This completes the Technology Review. Return to the Main Menu and select the next topic.

SECTION 3: APPLICATIONS

Scene 3.1: Section Objectives

In this section we will consider:

- Why organizations should consider using smart cards
- The key advantages of smart card technology
- The current obstacles to acceptance of smart card technology, and
- Examples of where smart cards are being used today.

Scene 3.2: Application Areas

The first chip cards were simple prepaid telephone cards implemented in Europe in the mid-1980s, using memory cards. Today, the major active application areas for microprocessor-based smart cards include: financial, communications, government programs, information security, physical access security, transportation, retail and loyalty, health care, and university identification. These are intersecting areas in that the smart card may carry applications from more than one area (for example, combining information and physical security access, or financial and retail/loyalty).

Scene 3.3: Why Consider Smart Cards?

A rule of thumb useful to organizations considering the incorporation of smart card technology into their operations states the following:

IF

- A portable record of one or more applications is necessary or desirable.
- The records are likely to require updating over time.
- The records will interface with more than one automated system.
- Security and confidentiality of the records are important.

THEN

The smart card is a feasible automation solution for making data processing and data transfer more efficient and secure.

Scene 3.4: Advantages of Smart Cards

The key advantages of smart card technology include:

- The capacity provided by the on-board microprocessor and data capacity for highly secure, off-line processing.

- Adherence to international standards, ensuring multiple vendor sources and competitive prices.
- Established track record in real world applications.
- Durability and long expected life span (guaranteed by vendor for up to 10,000 read/writes before failure).
- Chip Operating Systems that support multiple applications and secure independent data storage on one single card.

Scene 3.5: Barriers to Acceptance of Smart Cards

The current obstacles to acceptance of smart card technology include:

- Relatively higher cost of smart cards as compared to magnetic stripe cards. (The difference in initial costs between the two technologies, however, decreases significantly when the differences in expected life span and capabilities--particularly in terms of supporting multiple applications and thus affording cost sharing among application providers--are taken into account.)
- Present lack of infrastructure to support the smart card, particularly in the United States, necessitating retrofitting of equipment such as vending machines, ATMs, and telephones.
- Proprietary nature of the Chip Operating System. The consumer must be technically knowledgeable to select the most appropriate card for the target application.
- Lack of standards to ensure interoperability among varying smart card programs.
- Unresolved legal and policy issues, such as those related to privacy and confidentiality, or to consumer protection laws.

Scene 3.6: Comparison with Magnetic Stripe Cards

The increasing complex performance and application requirements of today’s card systems have spurred interest in smart cards as an alternative to magnetic stripe cards, or as an enhancement to magnetic stripe cards in the form of a *hybrid card*. A hybrid card supports more than one technology as, for example, a smart card micro-module and a magnetic stripe.

Scene 3.7: Applications Areas

Shown below are examples of smart card applications. Click each application for an explanation.

Financial Applications

- Electronic Purse to replace coins for small purchases in vending machines and over-the-counter transactions.
- Credit and/or Debit Accounts, replicating what is currently on the magnetic stripe bank card, but in a more secure environment.
- Securing payment across the Internet as part of Electronic Commerce.

Communications Applications

- The secure initiation of calls and identification of caller (for billing purposes) on any Global System for Mobile Communications (GSM) phone.
- Subscriber activation of programming on Pay-TV.

Government Programs

- Electronic Benefits Transfer using smart cards to carry Food Stamp and WIC food benefits in lieu of paper coupons and vouchers.
- Agricultural producer smart marketing card to track quotas.

Information Security

- Employee access card with secured passwords and the potential to employ biometrics to protect access to computer systems.

Physical Access

- Employee access card with secured ID and the potential to employ biometrics to protect physical access to facilities.

Transportation

- Drivers Licenses.
- Mass Transit Fare Collection Systems.
- Electronic Toll Collection Systems.

Retail and Loyalty

- Consumer reward/redemption tracking on a smart loyalty card, that is marketed to specific consumer profiles and linked to one or more specific retailers serving that profile set.

Health Card

- Consumer health card containing insurance eligibility and emergency medical data.

University Identification

- All-purpose student ID card, containing a variety of applications such as electronic purse (for vending and laundry machines), library card, and meal card.

Scene 3.8: Applications in the U.S.

Because of the significant investment in an extensive magnetic stripe-based infrastructure, and the availability of reliable and low cost on-line telecommunication services, the U.S. has thus far represented a limited smart card market. Smart card projects implemented in the U.S. have been primarily closed systems deployed on military bases, universities, and corporate campuses. The exception to this has been the movement by the Federal Government to use smart cards in Electronic Benefits Transfers for food stamps and other similar social programs nationwide.

The Federal Government's ultimate goal is to adopt a limited number of multi-application smart cards that will support a wide range of Government-wide and agency-specific services. It is envisioned that eventually every Federal employee will carry smart cards that can be used for multiple purposes such as identification, building access, network access, property accountability, travel, and other administrative and financial functions.

The U.S. Smart Card market comprises six major industries. Financial services lead it off with 32% of the market. Followed by retail with 27%, government with 22%, education with 18%, and a tie for last between transportation and phone; both at 1%.

This completes Smart Card Technology, an on-line multimedia presentation, presented by the General Services Administration. We hope you have enjoyed this presentation and you will take time to explore the SmartGov Web site where you will find the latest in smart card news and information.